경운대학교 정보보안관리규정

제1장 총칙

제1조(목적) 이 규정은 경운대학교(이하 "우리대학교"라 한다)의 정보보안을 위하여 수행하여야 할 기본활동 규정을 목적으로 한다.

제2조(적용범위) ① 이 규정은 우리대학교 내의 모든 기관(부서) 및 전 교직원에게 적용한다.

② 이 규정에 없는 사항은 교육부 「정보보안기본지침」을 준용한다.

제3조(용어정의) 이 지침에 사용하는 용어의 정의는 다음과 같다.

1. “정보시스템”이란 서버, PC 등 단말기, 휴대용기억매체, 네트워크 장치, 응용프로그램 등 정보의 수집, 가공, 검색, 송수신에 필요한 하드웨어 및 소프트웨어를 말한다.
2. “정보자산”이란 정보 및 정보시스템을 통칭하며, 정보시스템에는 서버, 네트워크, 보안시스템, 시설 등이 포함된다.
3. “위협”이란 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인 또는 행위를 말한다.
4. “취약성”이란 자산의 잠재적 속성으로 위협의 이용 대상이 되는 것을 말한다.
5. “보안시스템”이란 정보의 수집, 가공, 저장, 검색, 송수신 중에 나타나는 정보의 훼손 변조 유출 등을 방지하기 위한 기술적 수단으로써 침입차단시스템, 침입탐지시스템, VPN(가상사설망)등이 이에 해당한다.
6. “정보통신실”이란 서버, PC등 전산장비와 네트워크 스위치, 라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말하며, 전산실, 통신실 및 전산자료 보관실 등을 말한다.
7. “저장매체”란 자기저장장치, 광저장장치, 반도체저장장치, 휴대용기억장치(USB등) 등 자료기록이 가능한 전자장치를 말한다.
8. “휴대용 저장매체”란 디스켓, CD, 하드디스크, USB 메모리 등 자료를 저장할 수 있는 것으로 정보시스템과 분리할 수 있는 기억장치를 말한다.
9. “정보보안” 또는 “정보보호”란 정보시스템 및 정보통신망을 통해 수집, 가공, 저장, 검색, 송수신 되는 정보의 유출, 위변조, 훼손 등을 방지하기 위하여 물리적, 관리적, 기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
10. “전자정보”란 대학 내 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
11. “사이버공격”이란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 방해 등 전자적 수단에 의하여 정보통신망을 불법 침입, 교란, 마비, 파괴하거나 정보를 절취, 훼

손하는 공격행위를 말한다.

12. “보안감사”란 정보보호 및 개인정보보호와 관련된 통제절차의 기록과 행동을 독립적으로 조사, 관할하고 관련 증거를 수집하여 분석함으로써 주요 정보자산의 무결성, 가용성 그리고 기밀성을 확보하고자 하는 일련의 정보보안 관리 활동을 말한다.

제2장 정보보안 기본활동

제4조(책무) 우리대학교 총장 및 정보보안담당관은 보유정보(전자정보를 포함)와 정보통신망을 보호하기 위한 보안대책을 마련하고 정보보안에 대한 책임을 진다.

제5조(정보보안조직의 구성 및 운영) ① 정보보안을 위한 조직으로 정보보안담당관, 정보보안담당자를 지정한다.

② 우리대학교 총장이 정보보안담당관에게 부여하는 기본활동은 다음 각 호와 같다.

1. 정보보안 정책 및 기본계획 수립·시행
2. 정보보안 관련 규정·지침 등 제·개정
3. 정보보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보보안 업무 지도·감독, 정보보안 감사 및 심사분석
5. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 수준진단
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집·분석 및 보안관제
9. 정보보안 사고조사 결과 처리
10. 정보보안 교육 및 정보협력
11. 주요 정보통신기반시설 보호활동
12. “사이버보안진단의날” 계획 수립·시행
13. 그 밖의 정보보안 관련 사항

③ 정보보안담당자에게 부여하는 기본활동은 다음 각 호와 같다.

1. 정보보안 계획(보안대책, 교육, 내부 감사, 예산 등) 수립 및 정보보안담당관 보고
2. 보안사고의 처리에 대한 분석 및 확인
3. 정보보안 관련 규정 및 기준의 신규 제정 및 개정업무 수행
4. 보안사고 발생 시 보안사고 분석, 사후관리 통제, 필요한 경우 대외기관 협조 요청
5. 신규 장비 및 시스템 도입 시 보안성 검토를 수행
6. 응용프로그램 개발 시 사전에 정의된 보안 요건에 따라 보안 적정성 검토
7. 정보보안관련 주요사항 정보보안담당관 보고
8. 서버, 네트워크, 보안시스템, 애플리케이션 및 DB 운영 등의 보안 실무를 담당
9. 교육부 사이버안전센터 위탁을 통한 보안관제 업무

10. 수립된 보안 계획에 따른 영역별 보안관리 이행 담당
11. 보안 인식 제고를 위한 제반 홍보 활동 수행
12. 보안사고 및 바이러스 사고 발생 시 이를 처리하고 그 결과를 관리
13. 각 지침에 따라 기타 정보보호 활동 및 세부수행 사항을 수행

제6조(정보보안심사위원회) ① 정보보안 업무의 효율적인 운영과 보안정책 수립, 심의 및 관리를 위하여 "정보보안심사위원회"(이하 "위원회"라 한다)를 둔다.

② 위원회 조직의 구성은 다음 각 호와 같다.

1. 위원장 : 기획처장
2. 위　원 : 위원은 전문성을 가진 교직원 중에서 위원장의 추천으로 총장이 위촉
3. 간　사 : 정보보안담당관

③ 위원회는 다음 각 호의 사항을 심의·의결한다.

1. 정보보안 관련 지침 수립 및 제·개정에 대한 사항
2. 분야별 보안대책의 수립에 관한 사항
3. 정보보안 위반자 심사 및 처리에 관한 사항
4. 정보보안업무 수행 상 조정과 협의를 필요로 하는 사항
5. 전산화 용역개발 사업과 관련된 정보보안에 관한 사항
6. 정보보안 위규자 심사 및 처리에 관한 사항
7. 기타 총장의 지시나 위원장이 필요하다고 인정하는 사항

제7조(정보보안 사고조사) ① 정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 하고 다음 각 호의 사항을 교육사이버안전센터나 정보보안담당관에게 통보한다. 이 경우, 사고원인 규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 안 된다.

1. 일시 및 장소
2. 사고 원인, 피해현황 등 개요
3. 사고자 및 관계자의 인적사항
4. 조치내용 등

② 총장은 재발방지를 위한 보안대책의 수립·시행 등 사고조사 결과에 따라 필요한 조치를 이행하고 필요시 결과를 교육부장관에게 제출한다.

제8조(정보보호 교육) ① 정보보안담당관은 자체 정보보안교육계획을 수립하여 연 1회 이상 전체 직원을 대상으로 관련 교육을 실시하여야 한다.

② 정보보안담당자는 전문성 제고를 위해 연간 15시간 이상 정보보안 교육을 이수한다.

③ 정보보안담당관은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안담당자 업무 전문성을 제고하기 위하여 노력하여야 한다.

제9조(사이버보안진단의날) ① 정보보안담당관은 매월 셋째 주 수요일에 “사이버보안진단의날”을 지정하고 자체점검을 통한 보안진단을 실시하여야 한다.

② 사용자는 자신의 컴퓨터에 "내PC지키미" 프로그램을 설치하고 실행하여 자체적으로 진단하고 진단결과 발견된 문제점을 조치하여야 한다.

③ 사이버보안진단날 보안점검을 수행하지 않는 이용자는 전산망 접속을 제한할 수 있다.

제10조(재난방지) ① 정보시스템을 운영하는 소속기관의 장은 인위적 또는 자연적인 원인으로 인한 정보시스템의 장애 발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대칙을 수립·시행한다.

② 백업데이터의 소실에 대비하여 일정분의 백업데이터는 원격지에 별도 보관하도록 한다.

제3장 정보보안 관리

제11조(인적보안) ① 정보통신망을 통하여 비밀 등 중요정보를 취급하는 사용자에 대해서는 비밀취급인가, 보안서약서 징구 등의 보안조치를 하여야 한다.

② 사용자가 보직변경 및 퇴직 등 인사이동이 있을 경우 관련 정보시스템 접근권한을 조정하여야 한다.

③ 외부 인력을 활용하여 정보시스템을 개발, 운용, 정비 등을 수행할 경우 해당 인력의 고의 또는 실수로 인한 정보유출이나 손실을 방지하기 위하여 보안조치를 수행하여야 한다.

제12조(정보시스템보안) ① 우리대학교에 필요한 일체의 정보시스템(서버, 네트워크장비, PC 등 포함)을 도입·사용할 경우, 사용자·시스템관리자 및 관리책임자를 지정 운용하여야 한다.

② 사용자는 개인 PC등 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련된 보안책임을 가진다.

③ 시스템관리자는 서버·네트워크 장비 등 정보시스템의 운용과 관련된 보안책임을 가진다.

④ 제1항 및 제3항과 관련하여 정보시스템을 실제 운용하는 부서의 장이나 과장 또는 팀장이 정보시스템 “관리책임자"가 되며, 관리책임자는 정보시스템 관리대장을 수기 또는 전자적으로 운용 관리하여야 한다.

⑤ 관리책임자는 해당 부서의 정보시스템 관리대장에 정보시스템의 최종 변경 현황을 유지 및 관리하여야 한다.

⑥ 정보보안담당관은 제1항이나 제5항에 명시된 정보시스템 운용과 관련된 보안 취약점을 발견하거나 보안대책 강구가 필요할 경우, 사용자·시스템관리자 및 관리책임자에게 시정을 요구할 수 있다.

제13조(PC등 단말기 보안관리) ① 단말기 사용자는 PC·노트북 등 단말기(이하 PC등) 사용과 관련된 일체의 보안관리 책임을 가진다.

② 정보보안담당관은 비인가자 PC등을 무단으로 조작하여 전산자료를 절취, 위·변조 및

훼손시키지 못하도록 다음 각 호의 보안대책을 단말기 사용자에게 인지 시키고, 사용자는 이를 준수하여야 한다.

1. PC등(CMOS 비밀번호), 자료(중요문서자료 암호화 및 비밀번호 설정), 사용자(로그온 비밀번호)등 비밀번호를 주기적으로 변경 사용한다.
2. 10분 이상 PC작업 중단 시 비밀번호가 적용된 화면보호기 설정
3. PC용 최신 바이러스 백신 운영·점검, 운영체제 방화벽 등을 운용하고 운영체제(OS) 및 응용프로그램(한글, 오피스, Acrobat 등)의 최신 보안패치 유지
4. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더 설정 금지
5. 메신저·P2P·웹하드 등 업무와 무관하거나 불필요한 Active-X등 보안에 취약한 프로그램과 비인가 프로그램·장치 설치 금지
6. 음란·도박·증권 등 업무와 무관한 사이트 접근 금지

③ 사용자는 PC등 단말기를 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 관리담당자와 협의하여 하드디스크에 수록된 자료가 유출·훼손되지 않도록 데이터 완전삭제 등 보안조치 하여야 한다.

④ 관리책임자는 사용자가 PC등을 기관 외부로 반출하거나 내부로 반입할 경우 최신 백신 등을 활용하여 해킹프로그램 및 웜·바이러스 감염여부를 점검하여야 한다.

⑤ 개인소유의 PC 등 단말기를 무단 반입하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 관리책임자의 승인을 받아 사용할 수 있다.

제14조(인터넷 PC 보안관리) ① 총장은 인터넷과 연결된 PC(이하 인터넷PC)를 비인가자가 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.

1. 메신저·P2P·웹하드 등 업무에 무관하거나 불필요한 Active-X 등 보안에 취약한 프로그램과 비인가 프로그램·장치의 설치 금지
2. 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용(단, 업무망과 인터넷망이 분리된 경우)
3. 음란·도박·증권 등 업무와 무관한 사이트 접근차단 조치

② 그 밖에 인터넷 PC의 보안 관리에 관련한 사항에 대해서는 제13조(PC 등 단말기 보안대책)를 따른다.

제15조(서버 보안관리) ① 서버 관리자는 서버를 도입·운용할 경우, 정보보안담당관과 협의하여 해킹에 의한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 한다.

② 서버 관리자는 서버 내 저장자료에 대해 업무별·자료별 중요도에 따라 사용자의 접근권한을 차등 부여하여야 한다.

③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제하여야 한다.

④ 서버 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거

하며 관리용 서비스와 사용자용 서비스를 분리 운용하여야 한다.

⑤ 서버 관리자는 서버의 관리용서비스 접속 시 특정 IP와 MAC 주소가 부여된 관리용 단말을 지정 운용하여야 한다.

⑥ 서버 관리자는 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비하여야 한다.

⑦ 서버관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시하여야 한다.

제16조(웹서버 등 공개서버 보안관리) ① 서버 관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치·운용하여야 한다.

② 정보보안담당관은 인터넷 관문 구간에 비인가자의 서버 저장자료 절취, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.

③ 서버 관리자는 비인가자의 공개서버 내에 비공개 정보에 대한 무단 접근을 방지하기 위하여 서버에 접근 사용자를 제한하고 불필요한 계정을 삭제하여야 한다.

④ 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해 사용된 도구(컴파일러 등)는 개발 완료 후 삭제를 원칙으로 한다.

⑤ 공개서버의 보안 관리에 관련한 그 밖에 사항에 대해서는 제15조(서버 보안관리)에 따른다.

제17조(홈페이지 게시자료 보안관리) ① 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 홈페이지 게시자료의 범위·방법등을 명시한 자체 홈페이지 정보공개 보안지침을 수립 시행하여야 한다.

② 사용자는 개인정보, 비공개 공문서 및 민감 자료가 포함된 문서를 홈페이지에 공개하여서는 아니 된다.

③ 사용자는 인터넷 블로그, 카페, 게시판, 개인홈페이지 또는 소셜 네트워크 서비스 등 일반에 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니 된다.

④ 정보보안담당관은 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 한다.

제18조(사용자 계정관리) ① 시스템관리자는 사용자에게 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자의 도용 및 정보통신시스템에 대한 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 사용자별 접근권한 부여
2. 외부인에게 계정 부여는 불허하되 업무상 불가피 할 경우 필요업무에 한해 특정기간 동안 접속하도록 하는 등 보안조치를 강구한 후 허용
3. 비밀번호 등 사용자 식별 및 인증 수단이 없는 사용자계정 사용 금지

② 시스템관리자는 사용자가 5회 이상에 걸쳐 로그인 실패 시 정보시스템 접속을 중단시키

도록 시스템을 설정하고 비인가자의 침입 여부를 확인 점검하여야 한다.

③ 시스템관리자는 교직원의 퇴직 또는 보직변경 발생 시 사용하지 않는 계정을 신속히 삭제하고, 특별한 사정이 없는 경우 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지하여야 한다.

제19조(비밀번호 관리) ① 사용자는 비밀번호 설정 사용 시 정보시스템의 무단사용 방지를 위하여 다음과 같이 구분하여야 한다.

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 정보시스템 사용자가 서버 등 정보통신망에 접속 인가된 인원인지 여부를 확인하는 사용자인증 비밀번호(2차)
3. 문서에 대한 열람、수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)

② 비밀이나 중요자료에는 자료별 비밀번호를 반드시 부여하되, 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.

③ 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

④ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제20조(네트워크 장비 보안관리) ① 시스템관리자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구해야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP、MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 최초 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안패치 실시
4. 불필요한 서비스 포트 제거

② 시스템관리자는 라우터 등 중요 네트워크장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자에 의한 침투 여부를 주기적으로 점검하여 정보보안담당관에게 관련 결과를 제출하여야 한다.

제21조(전자우편 보안대책) ① 사용자는 메일에 포함된 첨부파일이 자동으로 실행되지 않도록 설정하고 첨부파일 다운로드 시 반드시 최신백신으로 악성코드 및 바이러스를 검사하여야 한다.

② 사용자는 출처가 분명하지 않거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹 메일로 의심되는 메일 수신시에는 즉시 정보보안담당관에게 연락하여야 한다.

③ 사용자는 전자우편을 사용하는 PC에 대하여 제13조(PC 등 단말기 보안관리)에 명시된 보안조치 사항을 따른다.

제22조(휴대용 저장매체 보안대책) ① 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하고 정보보안담당관의 승인을 받아야 한다.

② 휴대용 저장매체를 사용할 경우 "휴대용 저장매체 관리대장"에 등록한 후 사용하여야 하며 업무목적 이 외 사적인 용도로 사용할 수 없다.

③ 휴대용 저장매체 관리책임자는 부서의 장, 또는 과장이나 팀장이 해당 부서 관리책임자가 된다.

④ 휴대용 저장매체 관리책임자는 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.

⑤ 휴대용 저장매체 관리책임자는 사용자가 USB 메모리를 PC 등에 연결 시 자동으로 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 검사하도록 한다.

⑥ 휴대용 저장매체를 폐기할 경우 데이터 완전 삭제를 시행한 후 관리대장에 처리 여부를 기록한다.

제23조(접근기록 관리) ① 시스템관리자는 정보시스템의 효율적인 통제·관리, 사고 발생 시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지 관리하여야 한다.

② 제1항의 접근기록에는 다음 각 호의 내용이 포함되어야 한다.

1. 접속자, 정보시스템·응용프로그램 등 접속 대상
2. 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

③ 시스템관리자는 접근기록을 분석한 결과, 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 정보보안담당관에게 즉시 보고하여야 한다.

④ 접근기록은 정보보안 사고발생 시 확인 등을 위하여 최소 6개월 이상 보관하여야 하며 접근기록 위·변조 및 외부유출 방지 대책을 강구하여야 한다.

제24조(정보시스템 개발 보안) ① 시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제
2. 개발시스템과 운영시스템의 물리적 분리
3. 소스코드 관리 및 소프트웨어 보안관리

② 시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 외부인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
3. 외부인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부인력에 의한 장비 반입·반출 및 자료 무단반출 여부 확인
5. 제1항의 제1호부터 제3호까지의 사항

③ 교내 홈페이지를 개발할 때 다음 각 호의 사항을 고려하여 안전한 웹사이트를 구축 및 개발하고 취약점 점검결과에 따른 조치결과를 정보보안담당관에게 승인을 득하여야 한다.

1. 홈페이지 개발 시 설계·구축 단계에서부터 정보보호를 고려하여 웹응용프로그램 개발 및 웹서버 구축
2. 교육부 사이버안전센터의 취약점 점검 후 점검결과에 따른 보안 취약점 제거 후 웹서비스 제공
3. 운영단계에서도 서버, 소프트웨어, 네트워크에 대한 지속적인 점검과 취약점 제거 등 정보보호 활동 수행
4. 교육부「정보보안기본지침」등 보안 관련 규정을 준수하고 한국인터넷진흥원 등 전문기관에서 발행한 보안관련 가이드 등을 참고하여 안전한 웹사이트를 구축 및 개발

④ 정보보안담당관은 제1항 및 제③항과 관련하여 보안대책의 적절성을 수시로 점검하고 정보시스템 개발을 완료한 경우에는 정보보안 요구사항을 충족하는지 검토하여야 한다.

제25조(정보시스템 유지보수) ① 정보보안담당관은 정보시스템 유지보수와 관련한 절차, 주기, 문서화 등에 관한 사항을 자체 규정에 포함하여야 한다. 유지보수 절차 및 문서화 수립 시 고려사항은 아래의 각 호와 같다.

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 유지보수를 위해 원래 설치장소 외 다른 장소로 정보시스템을 이동할 경우, 통제수단을 강구한다.
4. 정보시스템의 유지보수 시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용 등을 기록·유지하여야 한다.

② 시스템관리자는 자체 유지보수 절차에 따라 정기적으로 정보시스템 정비를 실시하고 관련 기록을 보관하여야 한다.

③ 시스템관리자는 정보시스템의 변경이 발생할 경우, 정보보안담당관과 협조하여 정보시스템의 설계·코딩·테스트·구현과정에서의 보안대책을 강구하며 정보보안담당관은 관련 적절성을 주기적으로 확인하여야 한다.

④ 정보보안담당관은 시스템관리자 등이 유지보수와 관련된 장비·도구 등을 반출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치 하여야 한다.

⑤ 시스템관리자는 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제26조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체, 반납, 폐기 등)하고자 할 경우에는 정보보안담당관의 승인 하에 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 자료를 삭제 할 경우 해당 정보가 복구될 수 없도록 완전삭제 하여야 한다.

제27조(정보통신시설 보안) ① 다음 각 호의 중요 정보통신시설 및 장소를 보호구역으로 설정 관리하여야 한다.

1. 전산정보센터 기기실
2. 그밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 인증·식별 등을 위한 출입문 보안장치(CCTV 등) 설치 및 주야간 감시
4. 휴대용 저장매체를 보관할 수 있는 용기 비치
5. 관리책임자 및 자료·장비별 취급자 지정 운용
6. 정전에 대비한 비상전원 공급 장치, 시스템의 안정적인 운영을 위한 전력관리 대책
7. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지 대책 등

제28조(무선랜 보안관리) ① 총장은 무선랜(와이파이 등)을 사용하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 정보보안담당관과 협의하여 보안심사위원회에 보안성 검토 심의를 의뢰하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보원장이 승인한 암호논리 사용)
2. MAC 주소 및 IP 주소 필터링 설정
3. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
4. 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

③ 시스템관리자는 제1항 및 제2항과 관련한 보안대책의 적절성을 수시로 점검·보완하여야 한다. 이 경우 정보보안담당관은 시스템관리자가 수행한 사항이 적절한지 확인하고 시정조치를 권고할 수 있다.

제29조(용역사업 보안관리) ① 정보보안담당관은 정보화·정보보호 사업을 외부용역으로 추진할 경우 사업 책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 용역사업 계약 시 계약서에 참가직원의 보안준수 사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지
3. 용역업체에 제공할 중요 자료는 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
4. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위해 복구가 불가능하도록 완전삭제
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
6. 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료 무단 반출 여부를 확인
7. 그 밖에 총장이 보안관리가 필요하다고 판단하는 사항

② 총장은「국가계약법」시행령 제76조 제1항 제18호에 따라 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부적당업자로 등록하여야 한다.

1. 우리대학교 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 이용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템(FW)·침입방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8.「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9.「개인정보보호법」제2조 제1호의 개인정보
10. 그 밖에 소속기관의 장이 공개가 불가하다고 판단한 자료

③ 그 밖의 사항에 대하여는「용역사업 보안관리 지침」을 참조한다.

제4장 정보보안사고 대응

제30조(보안사고) ① 보안사고의 범위는 비밀정보의 누설 또는 분실, 중요시설 및 장비의 파괴, 보호구역에 대한 불법침입 등이며, 다음 각 호와 같다.

1. 전산정보센터 및 각 건물의 장비 통신실 파괴, 정보통신망의 해킹
2. 악성 바이러스 유포 및 비밀번호 파일 유출
3. 응용프로그램 불법 복제 및 사용
4. 중요 정보의 유출, 파괴, 변조, 보안시스템 손괴 등

② 보안사고가 발생하였을 경우 사고를 발생하였거나 이를 인지한 자는 즉시 정보보안담당관 및 부서 관리책임자에게 보고하여야 한다.

제31조(보안사고 대응) ① 정보보안담당관은 보안사고가 발생했을 때 이에 대한 효율적인 처리 및 복구대응체계를 갖추고 그 피해를 최소화 하고 사고대응을 시행하여, 이행 실태를 지속적으로 확인 점검하여야 한다.

② 정보보안담당관은 사고조사를 실시하고 동일유형의 사고가 발생하지 않도록 제반 보안조치를 취한다.

부 칙

1. **(시행일)** 이 규정은 2014년 3월 1일부터 시행한다.

부 칙

1. **(시행일)** 이 규정은 2018년 12월 1일부터 시행한다.